

# FortiAuthenticator RADIUS Accounting with SSO for FortiOS 5.2.4 Design Guide

**VERSION 3.0**

Contents

Introduction.....3

Audience.....3

RADIUS Overview .....3

    Clarification of Terms .....3

FAC RADIUS Accounting Overview .....4

Protected EAP with MS-CHAPv2 Overview .....5

FortiAuthenticator Configuration.....6

    Enable FAC to LDAP Integration .....7

    Enable FAC as a source of Single Sign-On.....8

    Import Groups From LDAP .....9

    Enable FAC RADIUS Accounting..... 10

FortiGate Configuration..... 11

    FGT to FAC Integration ..... 11

    FGT Group Selection..... 11

    FGT Identity-Based Policy Using Group Imported From FAC ..... 12

    FGT to NPS Integration ..... 12

Microsoft Network Policy Server (NPS)..... 13

    RADIUS Clients and Remote RADIUS Server Groups..... 13

    RADIUS Connection and Network Policies ..... 15

Client Configuration..... 18

FAC RADIUS Accounting to SSO Verification and Troubleshooting..... 21

## Introduction

The purpose of this design guide is to provide a validated working configuration of FortiAuthenticator RADIUS Accounting to SSO. FortiAuthenticator supports the ability to receive RADIUS Accounting Packets and use the RADIUS Attribute Value Pairs as a source of authentication information and then push these events into FSSO. The components used are:

- FortiGate (FortiOS 5.2.4)
- Windows Server 2012 R2 with Network Policy Server
- FortiAP (v5.2-build0245)
- FortiAuthenticator v3.00-build0182-20150717-patch00
- Windows 7 SP1 laptop supporting 802.1X wireless authentication

This guide assumes that Virtual Domains are not enabled on the FortiGate and that Certificate Services are installed on the Network Policy Server. A Root CA is required because the CA public key is an integral part of 802.1x and will not work without it. This guide is also intended for medium to enterprise-sized environments that have a FortiAuthenticator (FAC). The FAC has better group management scalability and other features versus just a FortiGate (FGT) with RSSO, see the Clarification of Terms section for a further explanation.

## Audience

This guide is written for network and security administrators who have a solid understanding for following areas:

- Microsoft Server 2012 and Network Policy (NPS) Server administration
- Configuring Protected EAP with MS-CHAPv2
- Windows 7 administration
- FortiOS administration with FAC integration
- Wireless Access Points (AP) configuration

## RADIUS Overview

### Clarification of Terms

‘RADIUS Single Sign-On’ or RSSO – A FortiOS feature which uses RADIUS accounting start/stop messages to extract information including username and IP Address. The group parameter (Class attribute) is used to match a local Fortigate RSSO Group containing the string we expect to receive from the RADIUS peer. RSSO does not lookup incoming user accounts against LDAP or any other authorization backend information, and does not therefore know what groups a given AD user is a member of. Hence an admin will need to manage totally separate identity groups versus FSSO even if the users are the same.

‘RADIUS Accounting’ – A FortiAuthenticator feature which also uses RADIUS accounting start/stop messages to extract information including username and IP Address. The FortiAuthenticator then queries an LDAP backend for a given username and retrieves all group memberships for that user. The FortiAuthenticator can then create standard FSSO Groups with that information allowing a FortiOS policy to remain identical to the Active Directory group naming structure. The main benefit, is it provides one set of unified FSSO Groups for identity based rules.

In summary of the above, RSSO does not equate to RADIUS Accounting as most environments ideally want to be using RADIUS Accounting, and thus a FAC, to avoid the complexity surrounding the management of two separate types of group identity.

## FAC RADIUS Accounting Overview

### Summary:

WPA2 Enterprise via 802.1x, PEAP/MSCHAPv2 sends User Login to NPS.

NPS validates Username and password.

NPS sends Start/Stop/Interim RADIUS packets details to the FAC.

FAC queries LDAP for user group information.

FAC sends updates to FGT via SSO.

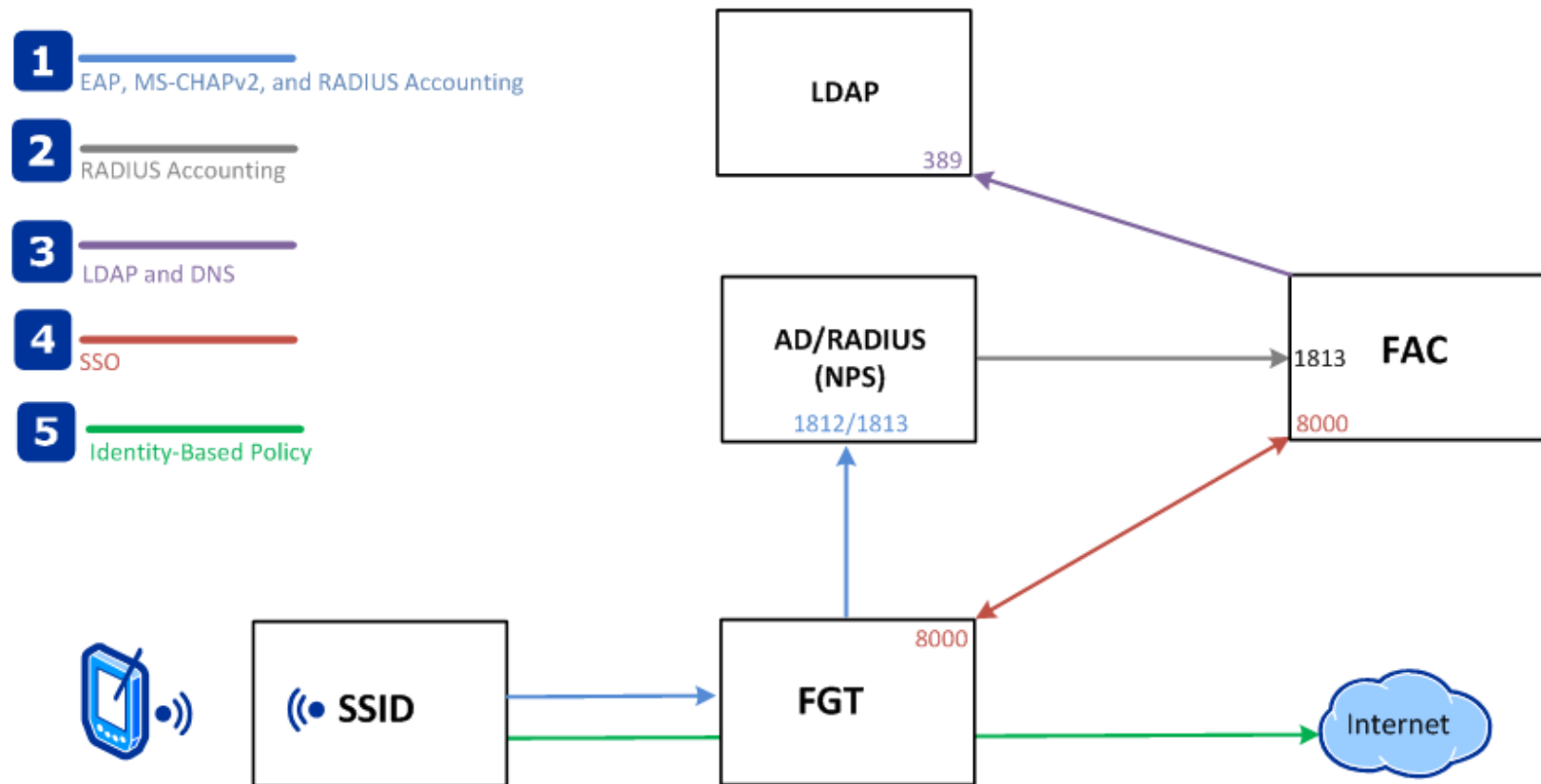


Figure 1

## Protected EAP with MS-CHAPv2 Overview

PEAP with MS-CHAP v2 is an EAP type that this design guide uses which is more easily deployed than Extensible Authentication Protocol with Transport Level Security (EAP-TLS) or PEAP-TLS because user authentication is accomplished by using password-based credentials (an Active Directory username and password) instead of digital certificates or smart cards. Only servers running Network Policy Server (NPS) and providing PEAP-MS-CHAPv2 authentication are required to have a certificate.

This next part is optional, the administrator can design to the solution to not use 'Server Validation' but involves more design consideration. When using Server Validation successful PEAP-MS-CHAP v2 authentication requires that the client trust the NPS server after examining the server certificate. For the client to trust the NPS server, the certification authority (CA) that issued the server certificate must have its own certificate in the Trusted Root Certification Authorities certificate store on the client computer. The server certificate used by NPS can be issued by your organization's private trusted root CA deployed on your network, or by a public CA, such as VeriSign or Thawte, that is already trusted by the client computer.

The diagram below shows a generic 802.1x authentication exchange. The WLC in our case is the FortiGate. The FortiAuthenticator is not shown, but it would communicate with NPS server for RADIUS Accounting packets which would be step 2 in Figure 1.

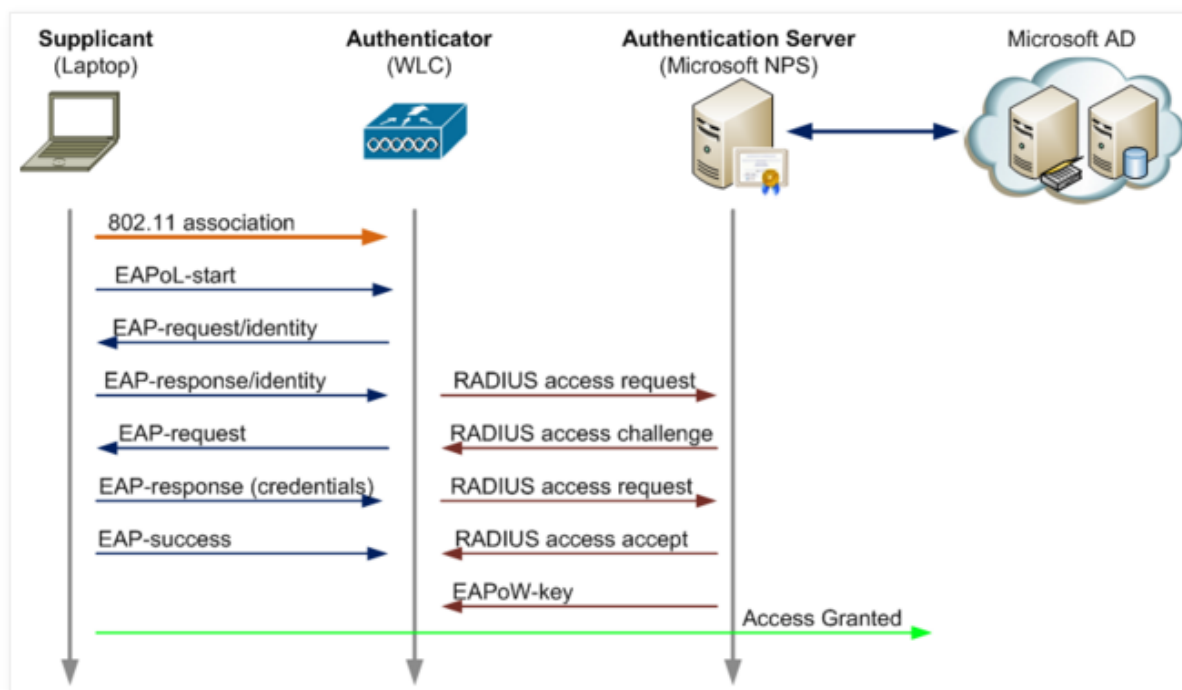


Figure 2

## FortiAuthenticator Configuration

Excluding the FortiAP profile which is outside the scope of this guide, but briefly described in the previous section, there are three main components required to support FAC RSSO Accounting functionality. Those components are specific to the FAC, FGT, and NPS. This guide also includes an optional step of Server Validation that the client performs against the NPS server as described in the PEAP section above.

The main configuration components we will be working with in the following sections are shown below:

1. FAC RSSO Accounting configuration
2. FGT to the FAC for SSO connectivity
3. NPS and FAC integration

At the conclusion of the steps listed above, the FAC will receive RADIUS Accounting details from NPS and the FGT will receive SSO details from the FAC. The FGT will also inherit SSO Groups directly from the FAC which will allow the replication of the actual LDAP group structure and can then be used to create identity based policies on the FortiGate.

A couple of notes to consider:

- FAC RADIUS Accounting is different to FAC RADIUS Accounting Proxy. The Accounting Proxy is not used or covered in this design guide, see the online RADIUS Accounting Proxy Guide for more information.
- If the FGT is providing DHCP services for the SSID instead of a DHCP Relay to a backend DHCP server, then the FGT will update NPS with RADIUS Accounting packets relating to the IP Address provided to wireless clients.

## Enable FAC to LDAP Integration

1. On the FAC, navigate to Authentication -> Remote Auth. Servers -> LDAP
2. Enter a Name, the 'Primary server name/IP' will be an Active Directory Global Catalog server. This relates to step 3 in Figure 1.

The screenshot shows the FortiAuthenticator web interface. On the left is a navigation menu with categories: System, Authentication, User Management, Self-service Portal, Remote Auth. Servers, and RADIUS Service. Under Authentication, there are sub-items: General, Lockouts, Passwords, Custom User Fields, LDAP (highlighted in red), and RADIUS. The main area is titled 'Edit LDAP Server'. It contains the following fields:

- Name: server2012
- Primary server name/IP: 192.168.10.3
- Port: 389
- ☐ Use secondary server
- Base distinguished name: DC=fortinetlab,DC=dyndns,DC=org (with a folder search icon)
- Bind type: ☐ Simple, ☒ Regular
- Username: CN=sysAdmin,CN=Users,DC=fortinetlab,DC=
- Password: (masked with dots)
- User object class: person
- Username attribute: samaccountname
- Group membership attribute: memberOf

Figure 3

3. Test the LDAP lookup functionality by clicking the folder search icon next to the 'Base distinguished name' in order to select a starting point in the LDAP tree for group and user queries.

The screenshot shows a 'Remote LDAP Browser' window. At the top, it says 'Remote LDAP Browser - Internet Explorer' and shows the URL 'https://10.0.20.2/ldap/browser/?\_popup=1'. The main area displays the LDAP server '192.168.10.3:389'. There is a 'Filter:' input field with 'Apply' and 'Clear' buttons. A checkbox 'Filter child nodes and show number of children' is checked. Below this is a tree view of LDAP objects:

- CN=Builtin (27)
- CN=Computers (3)
- OU=Domain Controllers (1)
- CN=ForeignSecurityPrincipals (4)
- CN=Infrastructure
- CN=LostAndFound
- CN=Managed Service Accounts
- CN=NTDS Quotas
- CN=Program Data (1)
- CN=System (25)
- CN=TPM Devices
- CN=Users (37)

At the bottom, there are fields for 'Distinguished name:' (DC=fortinetlab,DC=dyndns,DC=org) and 'Organization:' ([ Please Select ]), along with 'OK' and 'Cancel' buttons.

Figure 4

## Enable FAC as a source of Single Sign-On

1. On the FAC browse Fortinet SSO Methods -> SSO -> General
2. Select 'Enable authentication' and enter a 'Secret key'. The key must match similar configuration on the FGT which will be done in a later step. This relates to step 4 in Figure 1.
3. Select 'Enable RADIUS Accounting SSO clients', and 'Use RADIUS realm as Windows Active Directory domain'. This relates to step 4 in Figure 1.
4. Select 'Restrict user groups to SSO groups list' and 'Active'. This relates to step 4 in Figure 1. With this setting, the only groups that the FGT sees are the ones the FAC imports from LDAP and adds under FAC 'SSO Groups'.

The screenshot displays the FortiAuthenticator web interface. On the left, a navigation tree under 'System' > 'Authentication' > 'Fortinet SSO Methods' shows 'SSO' selected, with 'General' highlighted. The main panel is divided into three sections:

- FortiGate**:
  - Listening port:** 8000
  - ☒ **Enable authentication**
  - Secret key:** [masked]
  - Login expiry:** 480 minutes
  - Extend user session beyond logoff by:** 0 seconds (0-3600)
  - ☐ **Enable NTLM authentication**
- Fortinet Single Sign-On (FSSO)**:
  - Maximum concurrent user sessions:** 0 [Configure Per User/Group]
  - Log level:** Debug
  - ☐ **Exclude SSO source IP addresses matching these patterns:**
  - ☐ **Enable Windows Active Directory domain controller polling**
  - ☒ **Enable RADIUS Accounting SSO clients**
  - ☒ **Use RADIUS realm as Windows Active Directory domain**
  - ☒ **Enable Syslog SSO** [Configure syslog sources]
  - ☐ **Enable FortiClient SSO Mobility Agent Service**
  - ☐ **Enable hierarchical FSSO tiering**
  - ☐ **Enable DC/TS Agent Clients**
  - ☐ **Restrict auto-discovered domain controllers to configured domain controllers**
  - ☒ **Enable Windows Active Directory workstation IP verification**
  - ☒ **Enable IP change detection via DNS lookup**
- User Group Membership**:
  - ☒ **Restrict user groups to SSO groups list**
  - Group cache mode:** ☐ Passive ☒ Active
  - Group cache update period for active logons:** 480 minutes (1-10080) [Update cache]
  - Base distinguished names to search for nesting of users/groups into cross domain, domain local groups:** [empty text area]

Figure 5



## Import Groups From LDAP

1. On the FAC, browse to Fortinet SSO Methods -> SSO -> SSO Groups and click 'Import'
2. Expand the LDAP tree (See 'Enable FAC to LDAP Integration' on page 7 for reference)
3. Whatever groups are selected here will be passed on to the FGT

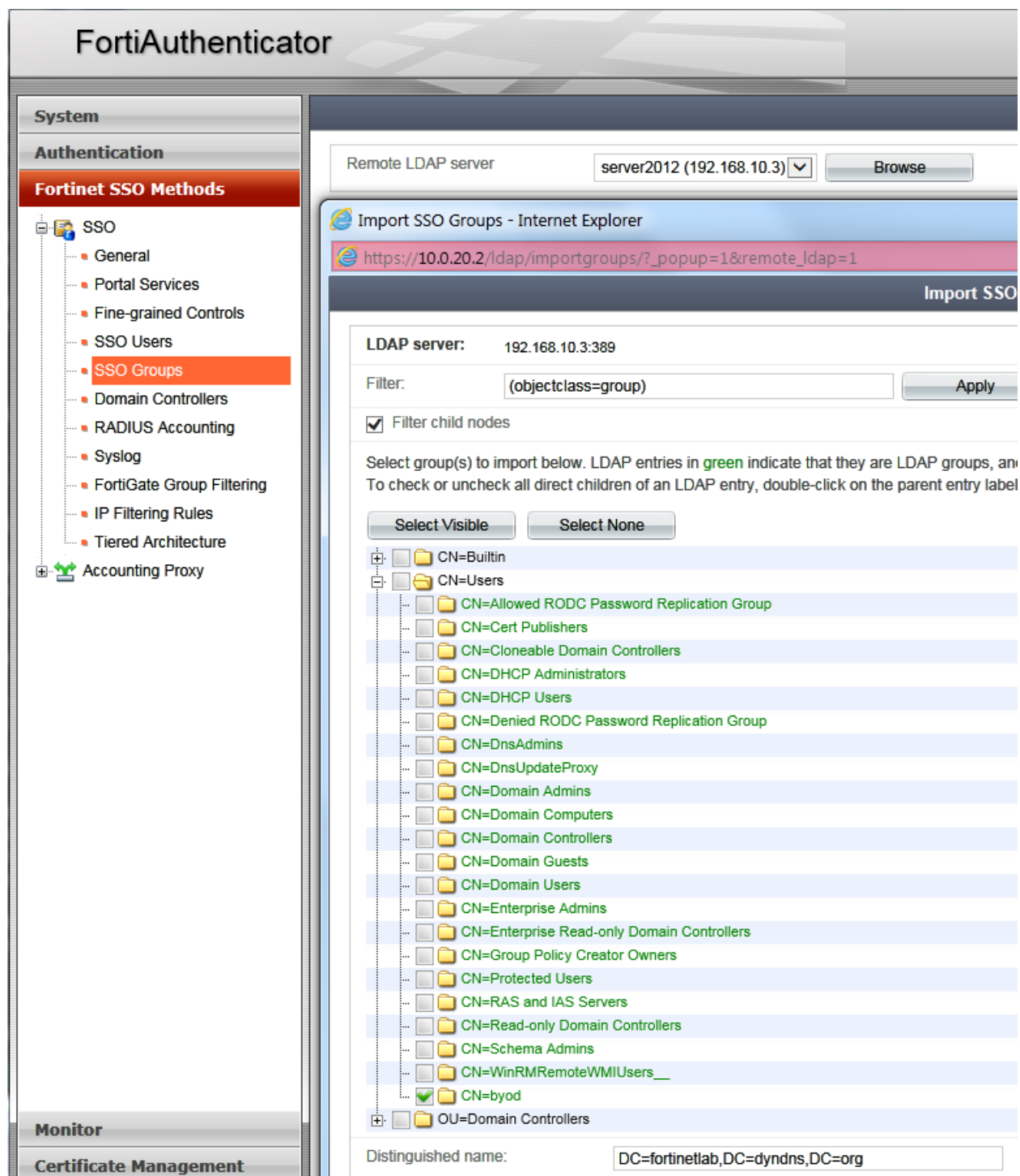


Figure 6

## Enable FAC RADIUS Accounting

1. On the FAC browse Fortinet SSO Methods -> SSO -> RADIUS Accounting
2. Enter a Name, the 'Client name/IP' will be the NPS, select 'SSO user type' 'Remote Users', and select 'Remote LDAP server' which was configured in the previous section. This relates to step 2 in Figure 1.
3. It is then necessary to configure NPS to forward RADIUS Accounting packets to the FAC which will be done in a later step. In order for FAC RADIUS Accounting to work, it is mandatory that the accounting packets contain the required Attribute Value Pairs (AVPs) which trigger an authentication event. The mandatory AVPs are:
  - Username = <User-Name>
  - Client IP = <Framed-IP-Address>

The screenshot displays the FortiAuthenticator web interface. On the left, a navigation tree under 'System' > 'Authentication' > 'Fortinet SSO Methods' shows 'RADIUS Accounting' selected. The main panel is titled 'FortiAuthenticator' and contains the following configuration fields:

Name:	NPS-to-FAC-Accounting	
Client name/IP:	192.168.10.4	
Secret:	••••••••	
Description:		
SSO user type:	<input type="radio"/> External <input type="radio"/> Local users <input checked="" type="radio"/> Remote users	
Remote LDAP server:	server2012 (192.168.10.3) [v]	

Below these fields is a section titled 'RADIUS Attributes' with the following configuration:

Username attribute:	User-Name	[Browse] [Default]
Client IP attribute:	Framed-IP-Address	[Browse] [Default]
User group attribute:	Fortinet-Group-Name	[Browse] [Default]

Figure 7

# FortiGate Configuration

## FGT to FAC Integration

1. On the FGT navigate to User&Device->Authentication->SingleSign-On and click 'Create New'
2. Enter a Name, and under 'Primary Agent IP/Name' enter the FAC details
3. Click 'Users/Groups' and the groups available should match exactly what was imported into the FAC see page 9 for reference. Any time the FAC groups sent to the FGT are changed, you need to click 'Apply&Refresh' shown below in order for the new groups to appear
4. Note, there is no need to select an LDAP server because the FGT is not doing any LDAP queries – the group information received is based on what the FAC is configured to send

**FORTINET** FortiGate VM64

**System**

**Router**

**Policy & Objects**

**Security Profiles**

**VPN**

**User & Device**

User

- User Definition
- User Groups
- Guest Management

Device

Authentication

Single Sign-On

**Edit Single Sign-On**

Name: FAC

Primary Agent IP/Name: 10.0.20.2 Password: .....

Secondary Agent IP/Name: Password: More FSSO agents

LDAP Server: Click to set...

Users/Groups: CN=BYOD,CN=USERS,DC=FORTINETLAB,DC=DYN...

**Apply & Refresh**

Figure 8

## FGT Group Selection

1. On the FGT navigate to User&Device->UserGroups, click 'Create New', select 'Fortinet Single Sign-On (FSSO)', click the '+' sign to add 'Members' – the group displayed will match what the FAC has selected from LDAP. The ones selected by the FAC are the only groups that will be made available to the FGT, see page 9 for reference

**FORTINET** FortiGate VM64

**System**

**Router**

**Policy & Objects**

**Security Profiles**

**VPN**

**User & Device**

User

- User Definition
- User Groups

**Edit User Group**

Name: byod

Type: ☐ Firewall ☒ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: CN=BYOD,CN=USERS,DC=FORTINETLAB,DC=DYN...

**OK**

Figure 9

## FGT Identity-Based Policy Using Group Imported From FAC

1. Create an Identity-Based Policy as usual

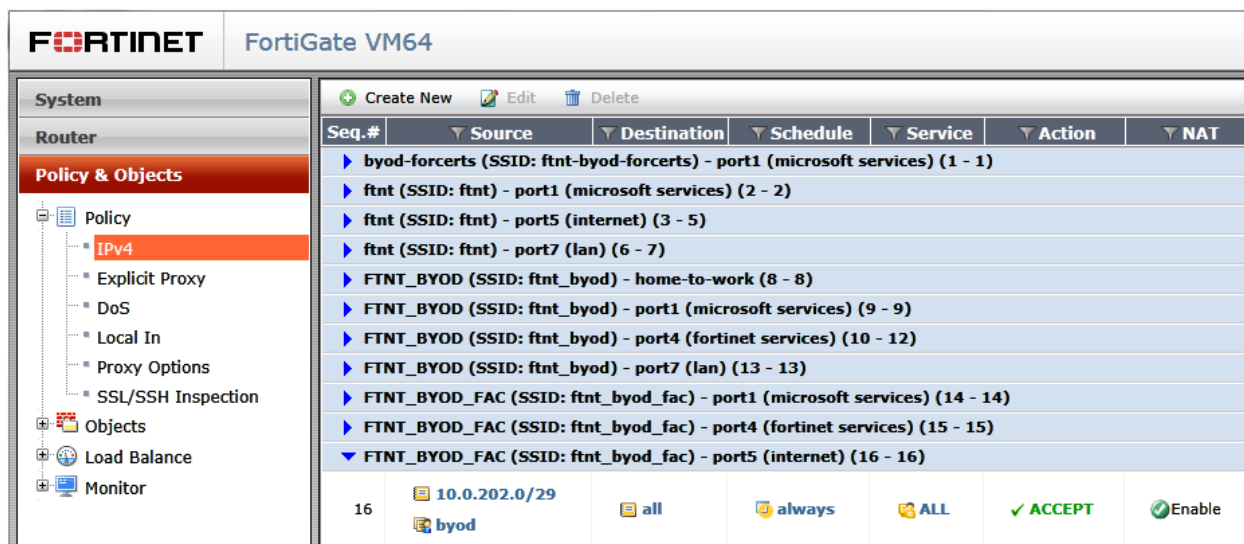


Figure 10

## FGT to NPS Integration

1. On the FGT navigate to User&Device -> Authentication -> RADIUS Servers, click 'Create New', and enter the NPS details. The 'Primary Server Secret' must match the NPS configuration for that setting. This related to step 1 of figure 1 and is what allows the WPA2 Enterprise wireless authentication to work.

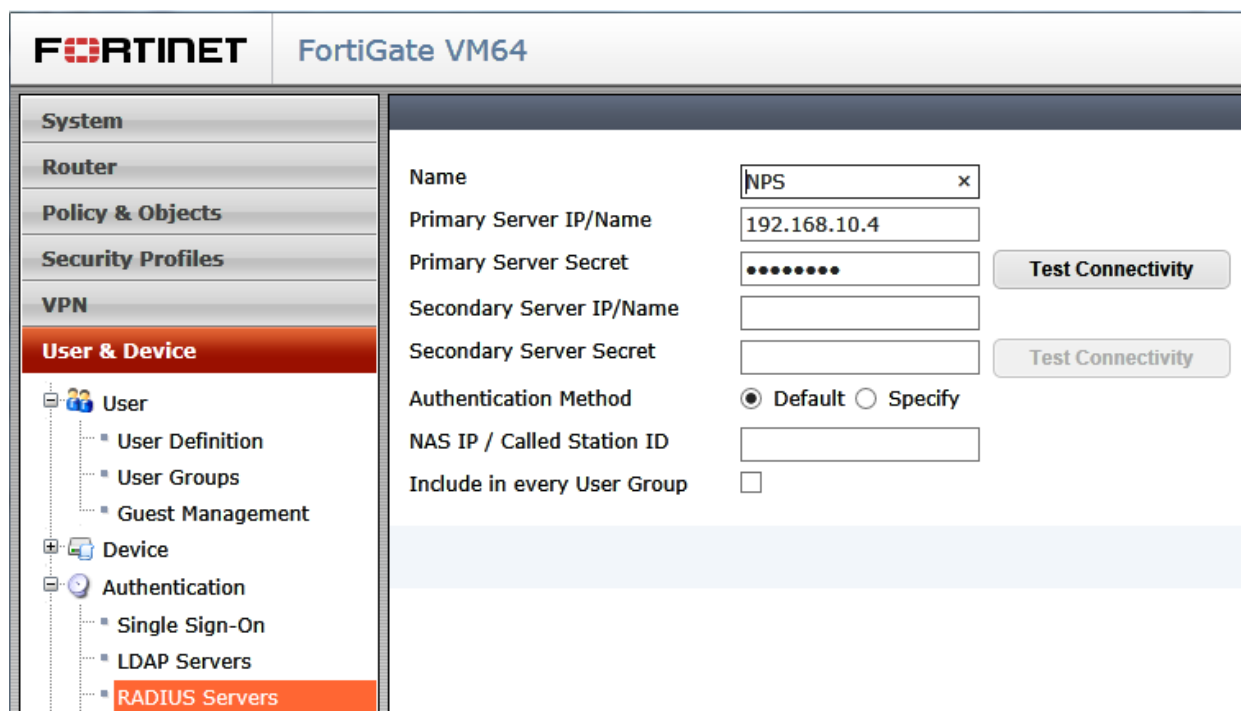


Figure 11

## Microsoft Network Policy Server (NPS)

The Microsoft NPS provides the authentication and accounting functionality in this environment. When a user provides login details to via the AP, the FGT will send those details via 802.1x to the NPS to verify the username and password against Active Directory. The NPS will then send RADIUS Accounting Packets to the FAC.

At the end of this section, the NPS will be configured to:

1. Authenticate users
2. Receive RADIUS Accounting packets from the FGT about the IP Address per wireless client
3. Send RADIUS Accounting packets to the FAC (see step 2 in Figure 1 for reference)

### RADIUS Clients and Remote RADIUS Server Groups

1. In the “Network Policy Server” click “NPS (Local) | RADIUS Clients and Servers”
2. Right-Click “RADIUS Clients” | Select “New” and enter “Friendly name” “IP Address” and “Shared Secret” which must match the FortiGate ‘Primary Server Secret’ entered in a previous section.

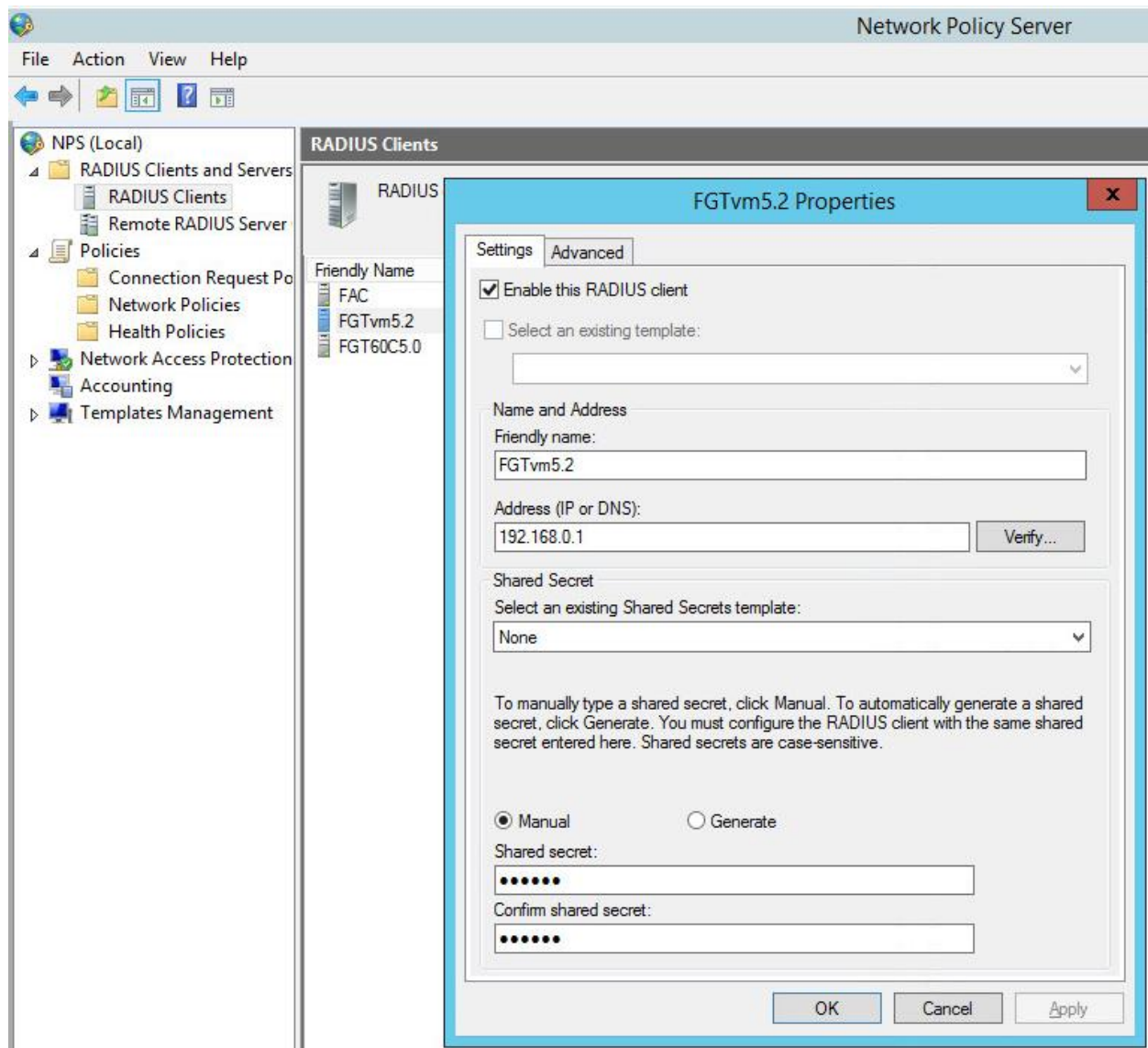


Figure 12

3. Right-Click 'Remote RADIUS Server Groups', select 'New' and enter the Group name and click 'Add'
4. Enter the FAC details accordingly.

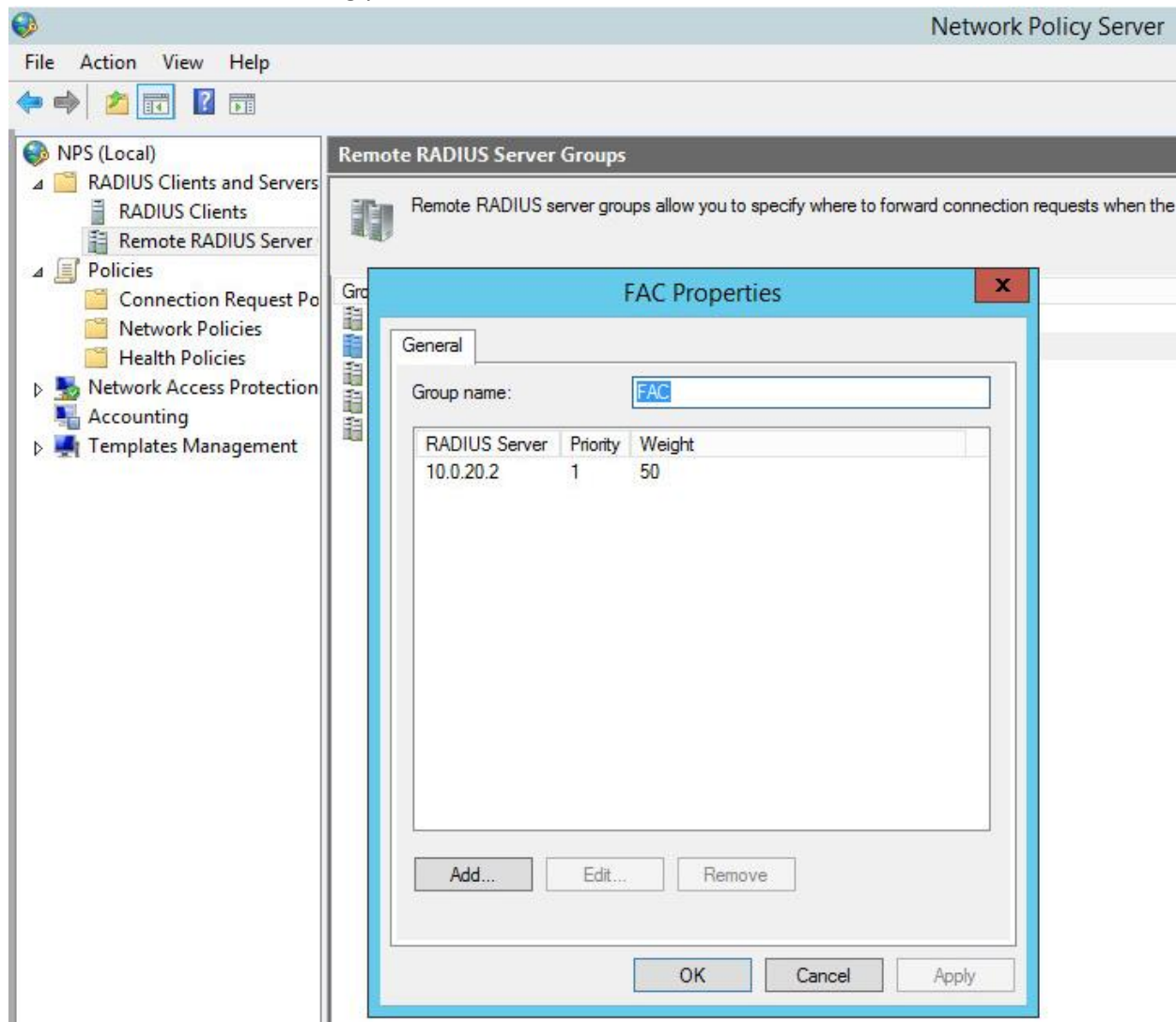


Figure 13

## RADIUS Connection and Network Policies

1. Right click 'Connect Request Policies' and create a new policy like what is shown below.
2. The 'Called Station ID' is the SSID from the FortiGate. Use the Called Station ID in this format 'SSID\$' in order to further control the policy selection
3. The 'Client IP Address' is the FortiGate interface that sends the 802.1x details on behalf of the wireless client.
4. It advisable to link the Connect Request and Network Policies with the Called Station ID and Client IP Address, because it helps ensure that the Connection and Network Policies are 'linked' which helps with scalability in large environments
5. The 'Accounting Provider Name' references the FAC configuration for 'Remote RADIUS Server Groups' from the previous page

The screenshot displays the Network Policy Server (NPS) console. The left pane shows the 'Policies' folder expanded, with 'Connection Request Policies' selected. The right pane shows the configuration for the 'FGT Connection Policy (ssid frnt\_byod\_fac)'.

**Connection Request Policies**

Connection request policies allow you to designate whether connection requests are processed by PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
FGT Connection Policy (ssid frnt_byod_fac)	Enabled	1	Unspecified
FGT Connection Policy (ssid frnt_byod)	Enabled	2	Unspecified
FGT60C5.0	Enabled	3	Unspecified
FGT60C5.0 (ssid ames_frnt)	Disabled	4	Unspecified
Use Windows authentication for all users	Disabled	999999	Unspecified

**FGT Connection Policy (ssid frnt\_byod\_fac)**

Conditions - If the following conditions are met:

Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 W
Client IPv4 Address	192.168.0.1
Called Station ID	frnt_byod_fac\$

Settings - Then the following settings are applied:

Setting	Value
Accounting Provider Name	FAC
Authentication Provider	Local Computer
Override Authentication	Disabled

Figure 14



6. Right click 'Network Policies' and enter a policy similar to what is shown below for 'Conditions' and 'Settings'.  
The 'Condition' settings relate to:
- User Groups = the LDAP group that contains users authenticating for wireless services
  - Client IPv4 Address = the FGT interface that sends the 802.1x on behalf of the wireless client
  - Called Station ID = is the SSID from the FortiGate. Use the SSID with a dollar-sign as the value
  - Authentication Method = EAP needs to link to the NPS server certificate for 802.1x to work properly. See Figure 15 for an example, select 'Microsoft: Protected EAP (PEAP)', highlight then click 'Edit' to select the certificate

The screenshot shows the Network Policy Server (NPS) console. On the left is a tree view with 'Policies' expanded, showing 'Network Policies'. The main pane displays the configuration for the selected policy, 'FGTvm5.2 Network Policy (ssid frnt\_byod\_fac)'.

**Network Policies**

Network policies allow you to designate who is authorized to connect to the network and the circumstance

Policy Name	Status	Processing Order	Access Type	Source
FGTvm5.2 Network Policy (ssid frnt_byod)	Enabled	1	Grant Access	Unspecified
FGTvm5.2 Network Policy (ssid frnt_byod_fac)	Enabled	2	Grant Access	Unspecified
FGT60C5.0 Network Policy (ssid ames_frnt)	Enabled	3	Grant Access	Unspecified

**FGTvm5.2 Network Policy (ssid frnt\_byod\_fac)**

Conditions - If the following conditions are met:

Condition	Value
User Groups	FORTINETLAB\byod
Client IPv4 Address	192.168.0.1
Called Station ID	frnt_byod_fac\$
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-2
NAS Port Type	Wireless - IEEE 802.11 OR Wireless - Other

Settings - Then the following settings are applied:

Setting	Value
Extensible Authentication Protocol Configuration	Configured
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
Authentication Method	EAP
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Framed-Protocol	PPP
Service-Type	Framed

Figure 15



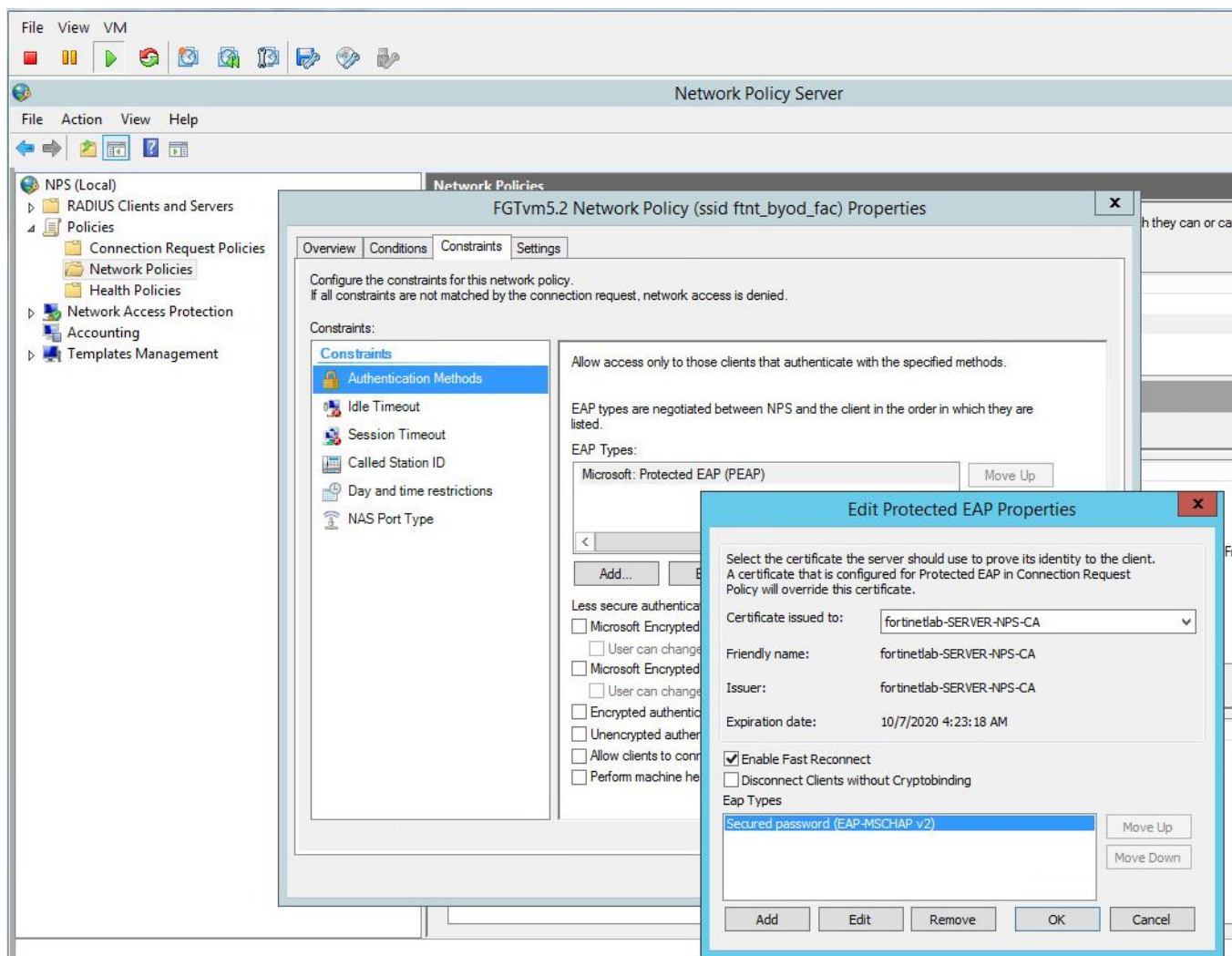


Figure 16

## Client Configuration

This section assumes that your 802.1x client is configured correctly in order to connect to an SSID using “WPA2 Enterprise” authentication. A Root CA is also required, but Server Validation is optional.

Below is an example of how the Windows 7 wireless network connection should look on a windows laptop running Window 7 SP1. Add a new wireless connection as shown in the following two images.

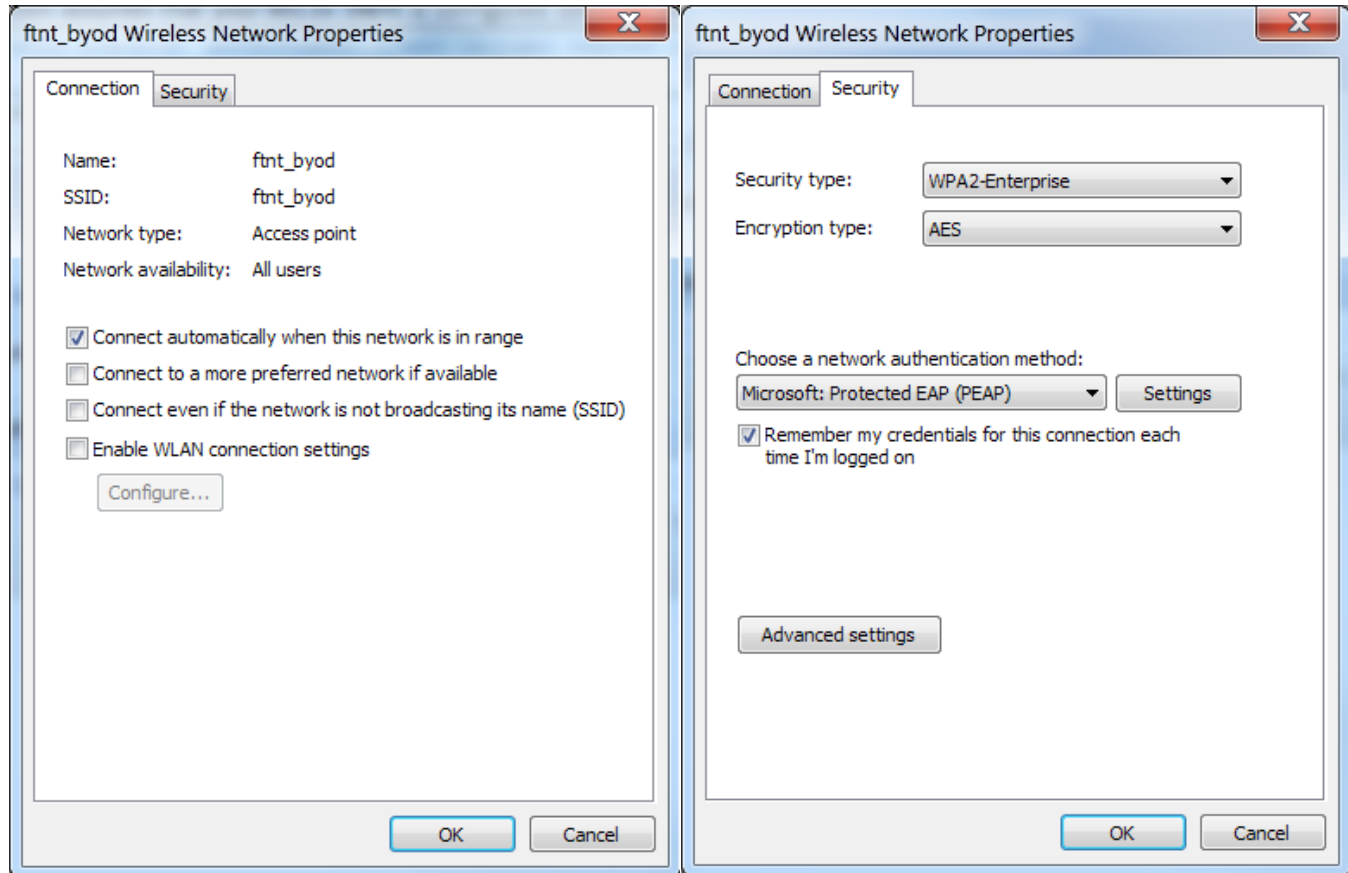


Figure 17

1. Click “Advanced settings”, select “Specify authentication mode” and select “User authentication”. Click ‘Save credentials’ to automate a wireless re-authentication anytime the user is in range. Be aware, that when the user changes passwords this will have to be updated.

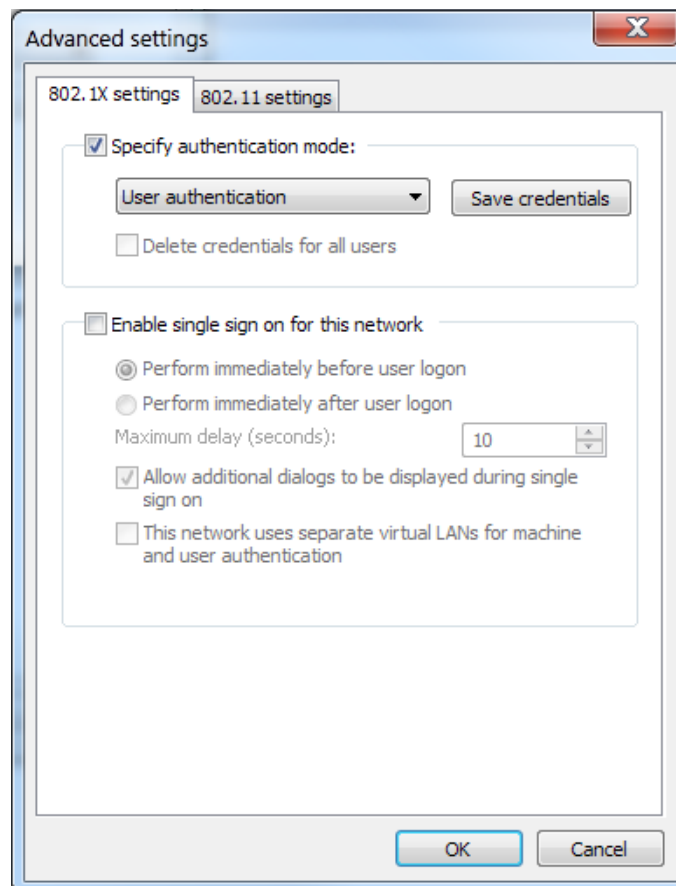


Figure 18

2. The following is an example of Server Validation where the wireless client verifies the certificate it's presented by the NPS server. This step is optional and is one of the most common errors/difficulties when using 802.1x. If "Validate server certificate" is selected then the Root CA certificate from the NPS must be added to the Trusted Root Certificate Store of the client. This can be done manually, via Group Policy in Active Directory, or by adding Certificate Services Web Enrollment to the NPS server along with an open SSID to allow clients to reach <https://192.168.0.1/certsrv> to download/install the certificate to the Trusted Root store.
3. Click "Configure..." and make sure that "Automatically use my Windows logon name and password" is not selected. This is also a main source of failure for clients as EAP will try to use the logon name/password of the local machine which is not the same as the users Active Directory credentials.

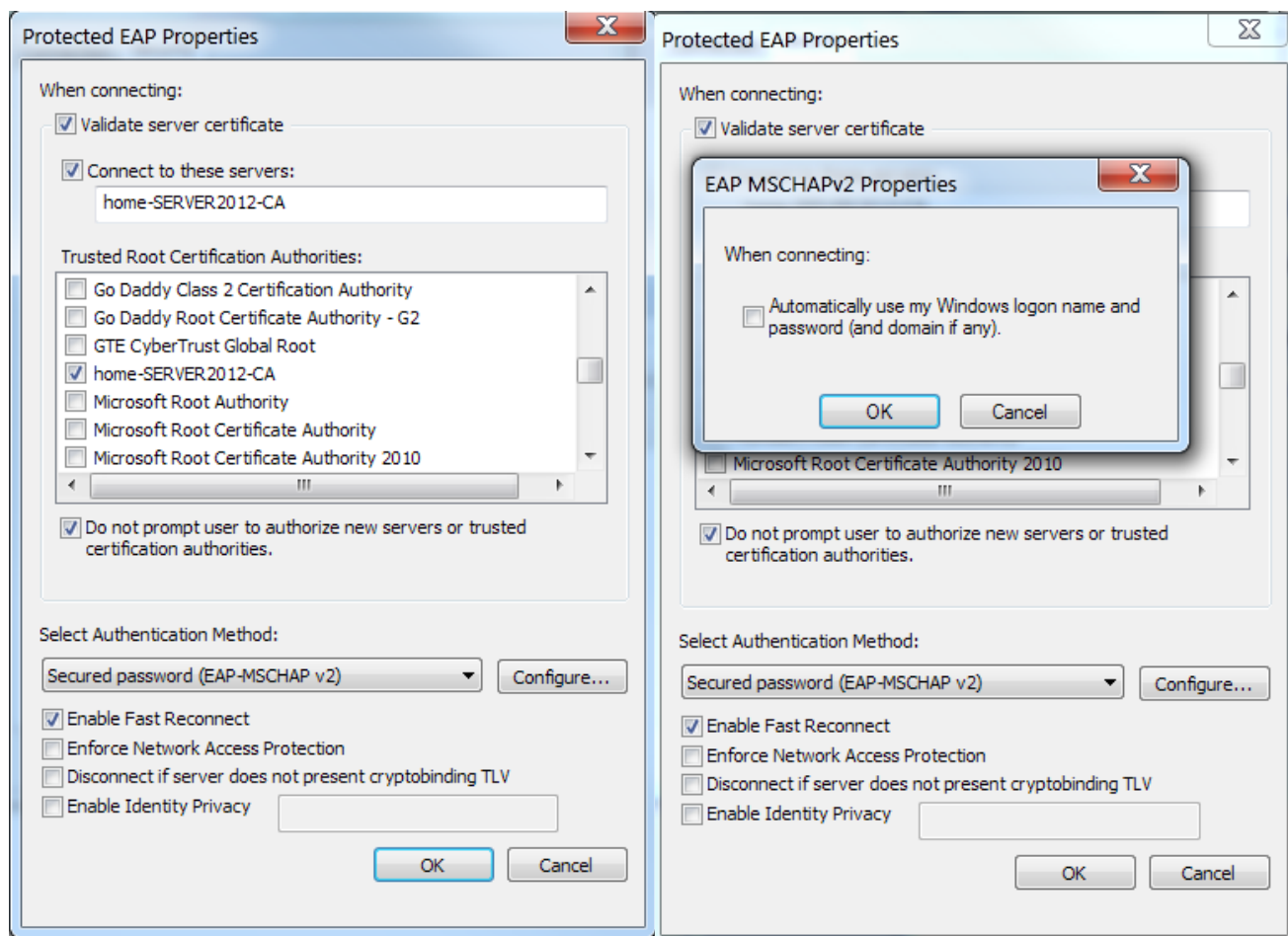


Figure 19

## FAC RADIUS Accounting to SSO Verification and Troubleshooting

1. This is an example of an Android mobile connecting to an WPA2 Enterprise SSID. The first task is to confirm with a packet sniffer that the FGT is connecting to NPS, and that NPS is connecting to FAC.

```
FGTvm-home # diag sniffer packet any 'port 1812 or port 1813' 4 50
interfaces=[any]
filters=[port 1812 or port 1813]
4.133392 port1 out 192.168.0.1.1029 -> 192.168.10.4.1813: udp 257 <-- FGT to NPS
4.134308 port1 in 192.168.10.4.61096 -> 10.0.20.2.1813: udp 267 <-- NPS to FAC
4.134326 port4 out 192.168.10.4.61096 -> 10.0.20.2.1813: udp 267
4.135517 port4 in 10.0.20.2.1813 -> 192.168.10.4.61096: udp 20
4.135524 port1 out 10.0.20.2.1813 -> 192.168.10.4.61096: udp 20
20.807236 port1 out 192.168.0.1.1031 -> 192.168.10.4.1812: udp 245
21.020201 port1 in 192.168.10.4.1812 -> 192.168.0.1.1031: udp 44
25.001154 port1 out 192.168.0.1.1030 -> 192.168.10.4.1812: udp 175
25.508790 port1 in 192.168.10.4.1812 -> 192.168.0.1.1030: udp 90
```

2. Wireshark conversion of step 1 showing successful MS-CHAPv2 via EAP tunnel from FGT to NPS. The NPS in this example is confirming a successful authentication.

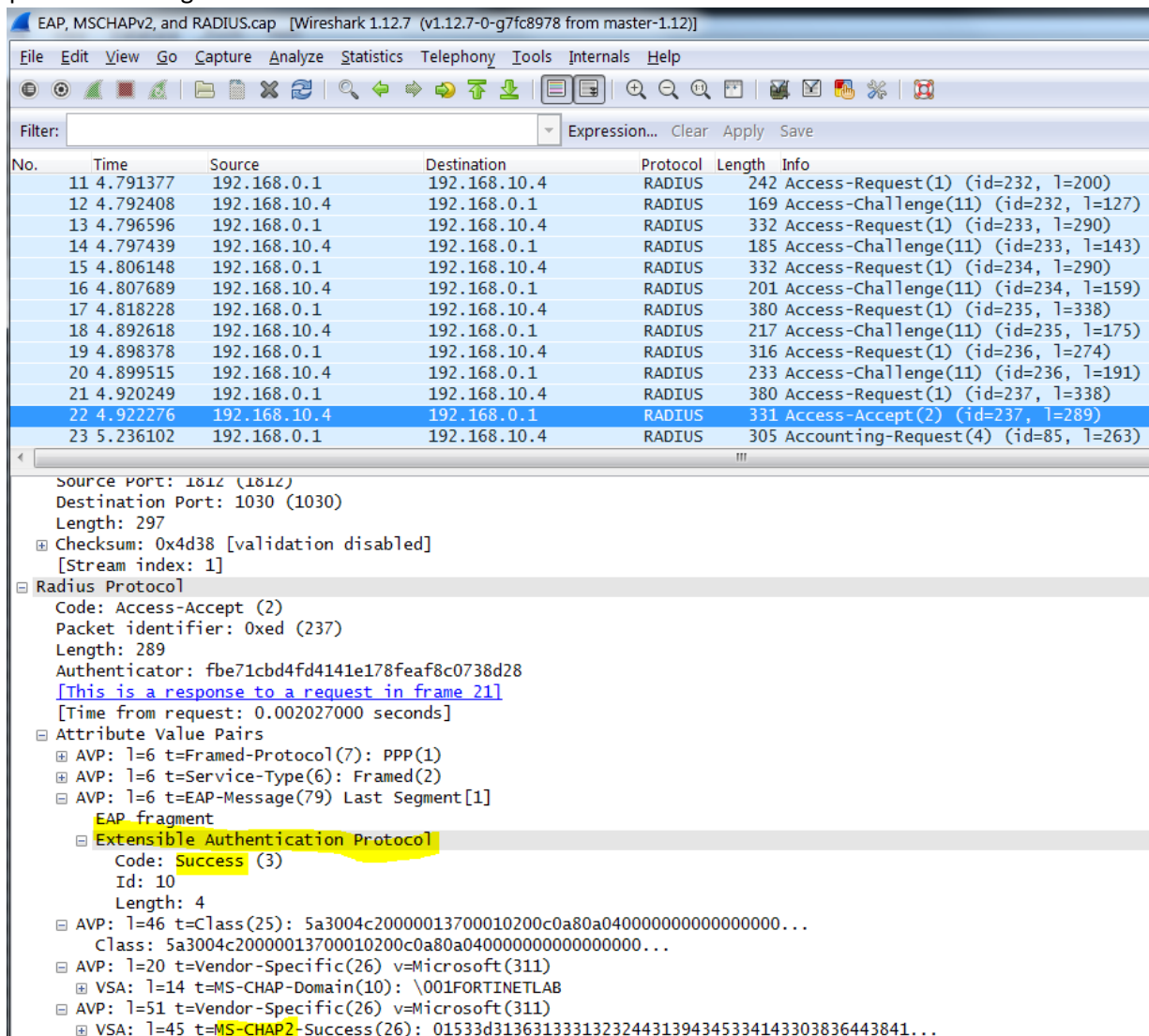


Figure 20

- Wireshark conversion of step 1 showing RADIUS Accounting from FGT to NPS. The FGT is not only forwarding port 1812 to NPS, but it's also initiating traffic on port 1813 to inform NPS of the Framed-IP-Address. If there are problems at this stage, ensure your FGT source-ip matches what the NPS expects, see to page 13 for reference. Notice the last line under 'Attribute Value Pairs --> 'Called-Station-Id', that is the SSID and MAC address from the FGT which is used in NPS Connection and Network Policies

EAP, MSCHAPv2, and RADIUS.cap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
11	4.791377	192.168.0.1	192.168.10.4	RADIUS	242	Access-Request(1) (id=232, l=200)
12	4.792408	192.168.10.4	192.168.0.1	RADIUS	169	Access-Challenge(11) (id=232, l=127)
13	4.796596	192.168.0.1	192.168.10.4	RADIUS	332	Access-Request(1) (id=233, l=290)
14	4.797439	192.168.10.4	192.168.0.1	RADIUS	185	Access-Challenge(11) (id=233, l=143)
15	4.806148	192.168.0.1	192.168.10.4	RADIUS	332	Access-Request(1) (id=234, l=290)
16	4.807689	192.168.10.4	192.168.0.1	RADIUS	201	Access-Challenge(11) (id=234, l=159)
17	4.818228	192.168.0.1	192.168.10.4	RADIUS	380	Access-Request(1) (id=235, l=338)
18	4.892618	192.168.10.4	192.168.0.1	RADIUS	217	Access-Challenge(11) (id=235, l=175)
19	4.898378	192.168.0.1	192.168.10.4	RADIUS	316	Access-Request(1) (id=236, l=274)
20	4.899515	192.168.10.4	192.168.0.1	RADIUS	233	Access-Challenge(11) (id=236, l=191)
21	4.920249	192.168.0.1	192.168.10.4	RADIUS	380	Access-Request(1) (id=237, l=338)
22	4.922276	192.168.10.4	192.168.0.1	RADIUS	331	Access-Accept(2) (id=237, l=289)
23	5.236102	192.168.0.1	192.168.10.4	RADIUS	305	Accounting-Request(4) (id=85, l=263)
24	5.236920	192.168.10.4	10.0.20.2	RADIUS	315	Accounting-Request(4) (id=51, l=273)

Frame 23: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits)

Ethernet II, Src: Vmware\_79:8d:c6 (00:0c:29:79:8d:c6), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.10.4 (192.168.10.4)

User Datagram Protocol, Src Port: 1029 (1029), Dst Port: 1813 (1813)

Source Port: 1029 (1029)

Destination Port: 1813 (1813)

Length: 271

Checksum: 0x94fe [validation disabled]

[Stream index: 2]

**RADIUS Protocol**

Code: Accounting-Request (4)

Packet identifier: 0x55 (85)

Length: 263

Authenticator: e7ca6d01adb733e7bb549f8b4129f315

**Attribute Value Pairs**

- AVP: l=19 t=Acct-Session-Id(44): 5619045A-00000438
- AVP: l=6 t=Acct-Status-Type(40): Start(1)
- AVP: l=6 t=Acct-Authentic(45): RADIUS(1)
- AVP: l=16 t=User-Name(1): mobile-android
- AVP: l=6 t=NAS-IP-Address(4): 0.0.0.0
- AVP: l=6 t=Framed-IP-Address(8): 10.0.202.6
- AVP: l=6 t=NAS-Port(5): 0
- AVP: l=33 t=Called-Station-Id(30): 12-09-0F-B8-36-A2:ftnt\_byod\_fac

Figure 21



4. Wireshark conversion of step 1 showing RADIUS Accounting from NPS to FAC. It includes the mandatory AVPs as described on page 10. When the FGT is providing DHCP services for wireless clients it will send Framed-IP-Address. If the FGT is a relay for DHCP, then the other DHCP server needs to provide this or the Framed-IP-Address will be missing and the FAC will discard the RADIUS Accounting packets.

EAP, MSCHAPv2, and RADIUS.cap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
11	4.791377	192.168.0.1	192.168.10.4	RADIUS	242	Access-Request(1) (id=232, l=200)
12	4.792408	192.168.10.4	192.168.0.1	RADIUS	169	Access-Challenge(11) (id=232, l=127)
13	4.796596	192.168.0.1	192.168.10.4	RADIUS	332	Access-Request(1) (id=233, l=290)
14	4.797439	192.168.10.4	192.168.0.1	RADIUS	185	Access-Challenge(11) (id=233, l=143)
15	4.806148	192.168.0.1	192.168.10.4	RADIUS	332	Access-Request(1) (id=234, l=290)
16	4.807689	192.168.10.4	192.168.0.1	RADIUS	201	Access-Challenge(11) (id=234, l=159)
17	4.818228	192.168.0.1	192.168.10.4	RADIUS	380	Access-Request(1) (id=235, l=338)
18	4.892618	192.168.10.4	192.168.0.1	RADIUS	217	Access-Challenge(11) (id=235, l=175)
19	4.898378	192.168.0.1	192.168.10.4	RADIUS	316	Access-Request(1) (id=236, l=274)
20	4.899515	192.168.10.4	192.168.0.1	RADIUS	233	Access-Challenge(11) (id=236, l=191)
21	4.920249	192.168.0.1	192.168.10.4	RADIUS	380	Access-Request(1) (id=237, l=338)
22	4.922276	192.168.10.4	192.168.0.1	RADIUS	331	Access-Accept(2) (id=237, l=289)
23	5.236102	192.168.0.1	192.168.10.4	RADIUS	305	Accounting-Request(4) (id=85, l=263)
24	5.236920	192.168.10.4	10.0.20.2	RADIUS	315	Accounting-Request(4) (id=51, l=273)
25	5.236931	192.168.10.4	10.0.20.2	RADIUS	315	Accounting-Request(4) (id=51, l=273)
26	5.237504	10.0.20.2	192.168.10.4	RADIUS	62	Accounting-Response(5) (id=51, l=20)
27	5.237514	10.0.20.2	192.168.10.4	RADIUS	62	Accounting-Response(5) (id=51, l=20)

Source Port: 61090 (61090)  
Destination Port: 1813 (1813)  
Length: 281  
Checksum: 0xe4c9 [validation disabled]  
[Stream index: 3]

**Radius Protocol**

Code: Accounting-Request (4)  
Packet identifier: 0x33 (51)  
Length: 273  
Authenticator: 78d24da0730b85c2eb8ab841046ec85e  
[\[The response to this request is in frame 26\]](#)

**Attribute Value Pairs**

- AVP: l=19 t=Acct-Session-Id(44): 5619045A-00000438
- AVP: l=6 t=Acct-Status-Type(40): Start(1)
- AVP: l=6 t=Acct-Authentic(45): RADIUS(1)
- AVP: l=16 t=User-Name(1): mobile-android
- AVP: l=6 t=NAS-IP-Address(4): 0.0.0.0
- AVP: l=6 t=Framed-IP-Address(8): 10.0.202.6
- AVP: l=6 t=NAS-Port(5): 0
- AVP: l=33 t=Called-Station-Id(30): 12-09-0F-B8-36-A2:ftnt\_byod\_fac
- AVP: l=19 t=Calling-Station-Id(31): 00-66-4B-B9-3D-78
- AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
- AVP: l=24 t=Connect-Info(77): CONNECT 11Mbps 802.11b

Figure 22

- The same information from step 1 can also be confirmed in the NPS Security Log. The most common error at this point is Connection Policy or Network Policy 'not matched'. If that happens, there is conflicting or missing information being received by NPS from the FGT. Adjust or correct the NPS policies as required.

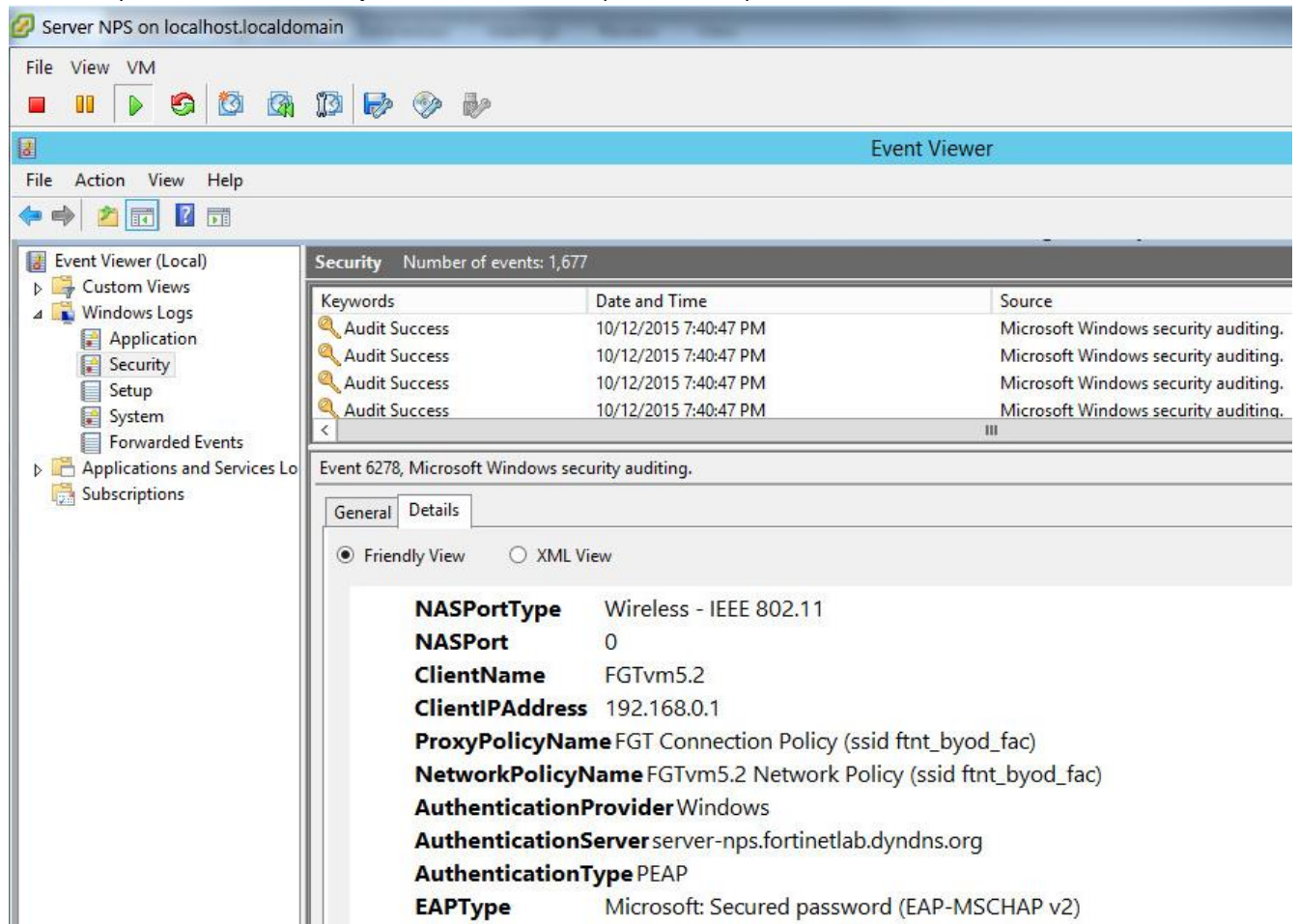


Figure 23



6. Run a 'tcpdump' on the FAC to confirm what it's seeing. Any FAC RADIUS Accounting problems can also be viewed via gui by pointing a browser to <https://10.0.20.2/debug> and selecting RADIUS Accounting from the pull-down menu. An authentication may be successful, but if the user is not found in LDAP (or LDAP is not configured correctly), the login will be received but the record will be dropped due to a lack of group information.

```
> tcpdump port 1813 -vv
tcpdump: listening on port1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:40:35.784818 IP (tos 0x0, ttl 125, id 21174, offset 0, flags [DF], proto UDP (17), length 301)
  192.168.10.4.61096 > 10.0.20.2.radius-acct: [udp sum ok] RADIUS, length: 273
    Accounting-Request (4), id: 0x33, Authenticator: 78d24da0730b85c2eb8ab841046ec85e
      Acct-Session-Id Attribute (44), length: 19, Value: 5619045A-00000438
        0x0000: 3536 3139 3034 3541 2d30 3030 3030 3433
        0x0010: 38
      Acct-Status-Type Attribute (40), length: 6, Value: Start
        0x0000: 0000 0001
      Acct-Authentic Attribute (45), length: 6, Value: RADIUS
        0x0000: 0000 0001
      User-Name Attribute (1), length: 16, Value: mobile-android
        0x0000: 6d6f 6269 6c65 2d61 6e64 726f 6964
      NAS-IP-Address Attribute (4), length: 6, Value: 0.0.0.0
        0x0000: 0000 0000
      Framed-IP-Address Attribute (8), length: 6, Value: 10.0.202.6
        0x0000: 0a00 ca06
      NAS-Port Attribute (5), length: 6, Value: 0
        0x0000: 0000 0000
      Called-Station-Id Attribute (30), length: 33, Value: 12-09-0F-B8-36-A2:ftnt_byod_fac
        0x0000: 3132 2d30 392d 3046 2d42 382d 3336 2d41
        0x0010: 323a 6674 6e74 5f62 796f 645f 6661 63
      Calling-Station-Id Attribute (31), length: 19, Value: 00-66-4B-B9-3D-78
        0x0000: 3030 2d36 362d 3442 2d42 392d 3344 2d37
        0x0010: 38
      NAS-Port-Type Attribute (61), length: 6, Value: Wireless - IEEE 802.11
        0x0000: 0000 0013
      Connect-Info Attribute (77), length: 24, Value: CONNECT 11Mbps 802.11b
        0x0000: 434f 4e4e 4543 5420 3131 4d62 7073 2038
        0x0010: 3032 2e31 3162
      Class Attribute (25), length: 46, Value: Z0..
        0x0000: 5a30 04c2 0000 0137 0001 0200 c0a8 0a04
        0x0010: 0000 0000 0000 0000 0000 0000 01d1 0417
        0x0020: 884b db68 0000 0000 0000 020b
      Vendor-Specific Attribute (26), length: 14, Value: Vendor: Fortinet (12356)
        Vendor Attribute: 23, Length: 6, Value: .fK.=x
        0x0000: 0000 3044 1708 0066 4bb9 3d78
      Vendor-Specific Attribute (26), length: 24, Value: Vendor: Fortinet (12356)
        Vendor Attribute: 24, Length: 16, Value: FAP21B3U13000175
        0x0000: 0000 3044 1812 4641 5032 3142 3355 3133
        0x0010: 3030 3031 3735
      Vendor-Specific Attribute (26), length: 12, Value: Vendor: Fortinet (12356)
        Vendor Attribute: 25, Length: 4, Value: V.r.
        0x0000: 0000 3044 1906 561b 7202
      Proxy-State Attribute (33), length: 10, Value: ....
        0x0000: c0a8 0a04 0000 0147
```

7. Successful WPA2 Enterprise logons should ultimately appear in the FAC log as 'RADIUS Accounting' events under Monitor -> SSO -> SSO Sessions and display under 'Source' as 'Radius Accounting'. Notice also, that the FAC has done an LDAP lookup for that use and all the groups will also display to the right of the 'Source' column.

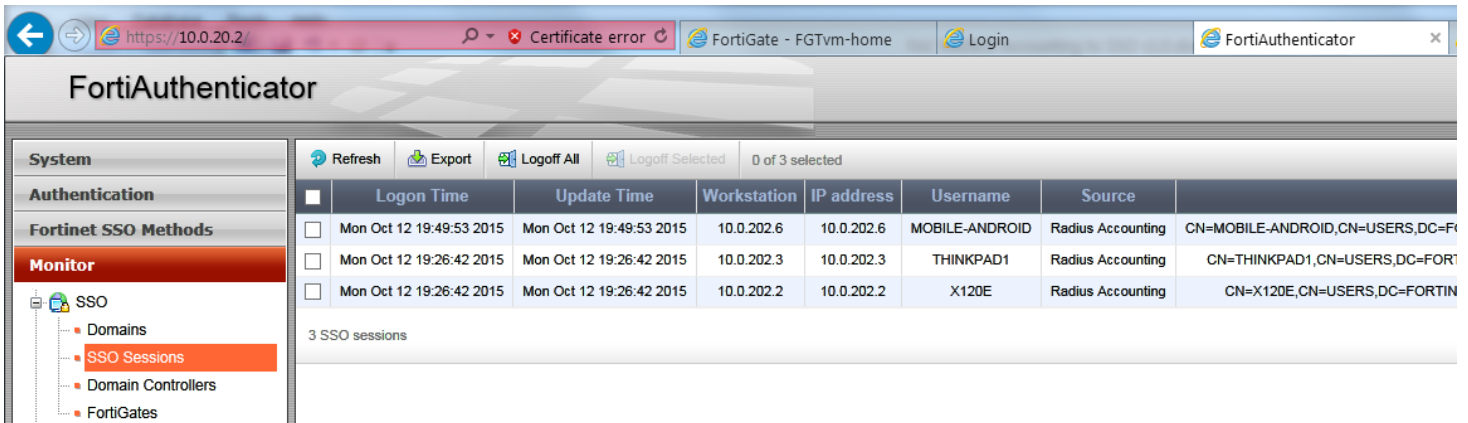


Figure 24

8. Those same events seen on the FAC as 'RADIUS Accounting' will appear on the FGT as 'FSSO' under User&Device -> Monitor -> Firewall but will display as 'Method' 'FSSO'.

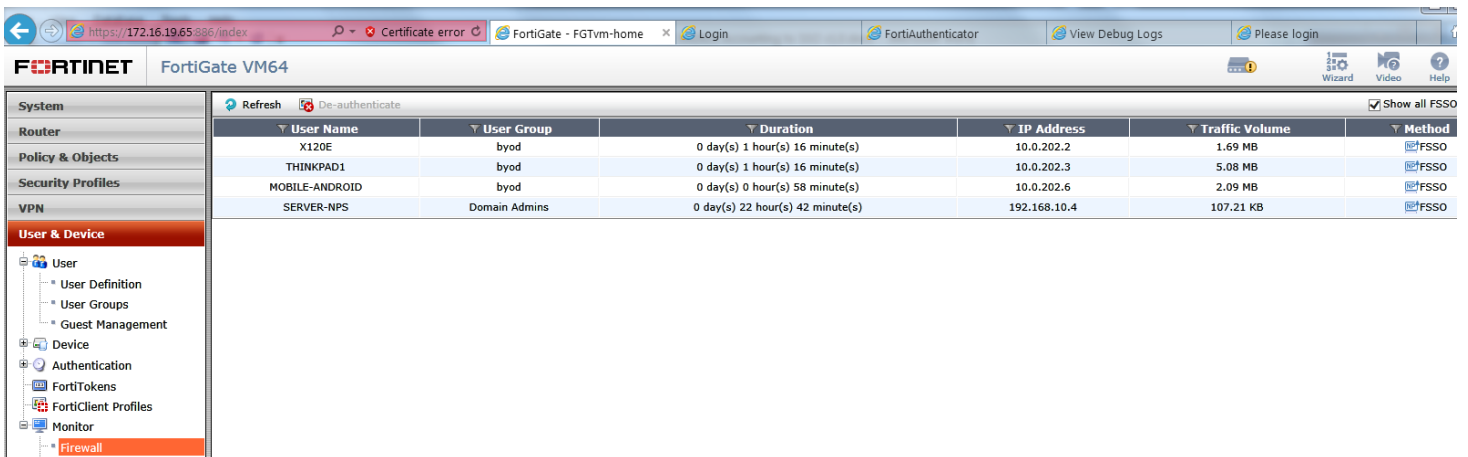


Figure 25

9. Some additional FGT cli commands to help with troubleshooting are shown below

```
FGTvm-home # diag firewall auth list
10.0.202.6, MOBILE-ANDROID
    type: fsso, id: 0, duration: 12, idled: 12
    server: FAC
    group_id: 3
    group_name: byod

FGTvm-home # diag debug app authd 8256
FGTvm-home # _event_read[FAC]: received heartbeat 0
_event_read[ControllerAgent]: received heartbeat 125628
_process_logon[FAC]: MOBILE-ANDROID(10.0.202.6) logged on with session id(0),
port_range_sz=0
```

-----End of Document-----



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.